GAO SURVEY, FEDERAL GOVERNMENT COMPUTER SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

OF THE

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY HOUSE OF REPRESENTATIVES

ONE HUNDREDTH CONGRESS

FIRST SESSION

MAY 19, 1987

[No. 15]

Printed for the use of the
Committee on Science, Space, and Technology

U.S. GOVERNMENT PRINTING OFFICE

74-579 WASHINGTON : 1987

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

H701-61

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

ROBERT A. ROE, New Jersey, *Chairman*

GEORGE E. BROWN, JR., California
JAMES H. SCHEUER, New York
MARILYN LLOYD, Tennessee
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
NORMAN Y. MINETA, California
BUDDY MacKAY, Florida
TIM VALENTINE, North Carolina
ROBERT G. TORRICELLI, New Jersey
RICK BOUCHER, Virginia
TERRY BRUCE, Illinois
RICHARD H. STALLINGS, Idaho
BART GORDON, Tennessee**
JAMES A. TRAFICANT, JR., Ohio
JIM CHAPMAN, Texas
LEE H. HAMILTON, Indiana
HENRY J. NOWAK, New York
CARL C. PERKINS, Kentucky
TOM McMILLEN, Maryland
DAVID E. PRICE, North Carolina
DAVID R. NAGLE, Iowa
JIMMY HAYES, Louisiana
DAVID E. SKAGGS, Colorado***

MANUEL LUJAN, JR., New Mexico*
ROBERT S. WALKER, Pennsylvania
F. JAMES SENSENBRENNER, JR., Wisconsin
CLAUDINE SCHNEIDER, Rhode Island
SHERWOOD L. BOEHLERT, New York
TOM LEWIS, Florida
DON RITTER, Pennsylvania
SID W. MORRISON, Washington
RON PACKARD, California
ROBERT C. SMITH, New Hampshire
PAUL B. HENRY, Michigan
HARRIS W. FAWELL, Illinois
D. FRENCH SLAUGHTER, JR., Virginia
LAMAR SMITH, Texas
ERNEST L. KONNYU, California
JACK BUECHNER, Missouri
JOEL HEFLEY, Colorado
CONSTANCE A. MORELLA, Maryland

HAROLD P. HANSON, *Executive Director*
ROBERT C. KETCHAM, *General Counsel*
REGINA A. SNYDER, *Chief Clerk*
R. THOMAS WEIMER, *Republican Staff Director*

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

DAVE McCURDY, Oklahoma, *Chairman*

DAN GLICKMAN, Kansas
BILL NELSON, Florida
TOM McMILLEN, Maryland
JIMMY HAYES, Louisiana

TOM LEWIS, Florida
ROBERT S. WALKER, Pennsylvania
F. JAMES SENSENBRENNER, JR., Wisconsin

---

*Ranking Republican Member.
**Resigned February 19, 1987 (H. Res. 89).
***Elected March 30, 1987 (H. Res. 133).

CONTENTS

WITNESS

May 19, 1987:

	Page
Thomas P. Giammo, Associate Director, Information Management and Technology Division, General Accounting Office	2

GAO SURVEY, FEDERAL GOVERNMENT COMPUTER SECURITY

TUESDAY, MAY 19, 1987

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY, SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS,

Washington, DC.

The subcommittee met, pursuant to notice, at 2:15 p.m., in room 2325, Rayburn House Office Building, Hon. Don Glickman (acting chairman of the subcommittee) presiding.

Mr. GLICKMAN. I think we'll go ahead and get started. I'm not Mr. McCurdy, but I used to be.

Today we'll take another look at computer security in the Federal Government, and I might mention that I believe tomorrow, the full Science Committee takes up a bill called the Computer Security Act, and I think we've worked out most of the bugs on this bill that will try to deal with some of the problems.

Our focus today will be a GAO audit requested by the committee, which has resulted in a report card on the security and privacy of unclassified information in nine developmental government computer systems. Many people will recall the outstanding predecessor study presented here in October, 1985. In that audit, GAO examined 25 operational computer systems at 18 federal agencies. Of course, the results varied widely. Some agencies measured up very well; others failed miserably. But the overall picture was a situation where many of the records that the government maintains on its citizens are vulnerable to unauthorized access and manipulation.

As a result of these troublesome findings, we asked GAO to determine if systems currently in various stages of development were any better. In other words, has the government improved its emphasis on security?

Today, the GAO will answer that question. It will also provide details as to where the specific weaknesses are, something we sought to avoid in the earlier study. In this instance, however, I feel it is important to expose any deficiencies in the new systems so that they may be addressed before the systems become operational.

I'd like to recognize Mr. Lewis, the ranking Republican.

Mr. LEWIS. Thank you, Mr. Chairman.

The extended use of computers in today's society has made abuse more widespread both in the private and the federal sectors. Consequently, today's hearing on the practices used by federal civil agen-

cies, and incorporating security controls in computer systems is very important.

This subcommittee has provided the Congressional leadership in exploring the federal commuter security needs, and I'd like to also comment and commend Mr. Glickman from Kansas for his tremendous work in this area, and I look forward to hearing from today's witnesses and the General Accounting Office on their most recent study of security controls and federal computer systems.

Mr. GLICKMAN. Thank you, Mr. Lewis.

Why don't we go ahead and have the folks from the GAO come up here to the desk. I know that we have Mr. Thomas Giammo, Associate Director of Information Management and Technology Division of the GAO, and Mr. Giammo, probably we would like for the record for you to identify who you're with.

We'd also point out that we do expect a vote within about five minutes, so we'll go and vote—we'll wait for the second bells and then we'll stop, go vote, and then we'll come back so you can proceed, realizing that we may have interrupted you in the middle of your statement.

Your prepared statement will be inserted immediately following your oral presentation.

Mr. Giammo?

STATEMENT OF THOMAS P. GIAMMO, ASSOCIATE DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, GENERAL ACCOUNTING OFFICE

Mr. GIAMMO. Mr. Chairman, members of the subcommittee, we are pleased to be here today to provide the subcommittee information on our review of the practices used by federal civilian agencies in identifying and incorporating appropriate security controls in automated information systems.

I have with me, Dr. Harold Podell, Group Director from the Information Management and Technology Division, and Mr. Ray Wyrsch, our Senior Attorney from our Office of General Counsel.

Mr. Chairman, the work we are reporting on today is a follow-on to the review of the information systems at 17 agencies that we performed at the request of this subcommittee in 1985. In that work, we examined the security of 25 automated information systems that had already been put into operation. We identified significant deficiencies in the controls of those systems that exposed them to abuse, destruction, error, fraud, and waste. An important finding of that work was that the origin of some of these deficiencies could be traced back to the development of the systems: appropriate security controls had not been successfully incorporated into many of the systems at the time they were planned, specified and built.

Our present review is in response to a July 30, 1985, request from the Chairman of this committee. We were requested to review how well civilian agencies are current assuring that appropriate security controls are being successfully incorporated into their mission-critical, sensitive systems that are now being developed.

Mr. Chairman, our review suggests that the practices currently being used by civilian agencies in the development of mission-criti-

cal, sensitive systems will not assure that the appropriate security controls are being successfully incorporated into these systems. Specifically, we reviewed the practices currently being used at nine civilian agencies in the development of nine specific systems. We found that the practices in use at all nine agencies had permitted decisions critical to the specification, design and construction of all nine systems to be made without adequate management consideration of important security issues.

Consequently, we believe that the systems currently in development at many civilian agencies, and intended to be used at least through the 1990's, are likely to possess many of the same security deficiencies we had previously found in the older systems already in operation. There is sufficient reason for concern that automated information systems of the future are likely to be at best only marginally better secured than those of the current generation. There is even more reason for concern, however, when one realizes that the automated information systems being developed today are likely to play an increasingly significant role in the essential business of our civilian agencies.

I would like to address the basis for these observations in greater detail, Mr. Chairman.

We began our review by surveying existing federal guidance relating to the practices that should be used in the development of federal information systems. On the basis of our initial analysis, we concluded that the body of existing guidance was not a suitable basis for assessing whether agency practices provided appropriate security controls during the development of systems. Most of the relevant civilian guidance addresses general aspects either of the development process or of security concerns—little effective guidance exists that comprehensively addresses how an agency should incorporate security considerations into the development process. This lack of good guidance is in itself a significant finding. We believe that this lack of specific federal guidance is an important contributing cause of the universality of the problems we found in this area.

So in conducting our review, rather than relying exclusively on the letter of existing federal guidance as the basis of our evaluation, we explicitly formulated our own criteria by applying the general principles given in that guidance to the specific activities needed to build security into an automated information system. In doing so, we followed accepted system development procedures.

The essence of these criteria turns out to be just common sense—we believe that agency management must consider security requirements and constraints when making critical decisions about overall system architecture, detailed design, testing, and implementation. Simply put, for each of the critical decision points in the development of an automated information system, we identified important security-related information that management should have prior to making those decisions. In our review, we checked to see if this information was available to management and if it was considered in reaching the critical system development decisions. Unless we had positive evidence of this, we judged that agency management's ability to assure that appropriate security controls were being incorporated was significantly reduced.

Not surprisingly, the criteria we used corresponds to the good practices set out in several individual agency guidance documents and a draft report of the President's Councils on Management Improvement, and the Council on Integrity and Efficiency.

Now, down to the specifics of the review. We reviewed the practices currently being used at nine agencies in the development of these nine specific mission-critical systems. And I will submit for the record, the identification of those systems.

[The identification of systems follows:]

NINE AGENCIES REVIEWED

Agency	System/subsystem
Immigration and Naturalization Service	Adjudications Casework System.
Farmers Home Administration	Automated Program Delivery System.
U.S. Customs Service	Automated Commercial System/Selectivity Module.
Veterans' Administration	Decentralized Hospital Computer Program/Blood Bank and Security Kernel Modules.
Federal Aviation Administration	Advanced Automation System.
International Trade Administration	Commercial Information Management System.
Social Security Administration	Claims Modernization Program/Release 3.1.
Internal Revenue Service	Automated Examination System.
Department of Energy	Strategic Petroleum Reserve System.

Mr. GIAMMO. We solicited informal agency comments from responsible officials on our findings at each agency. We received informal comments from seven of the nine agencies. But we have not yet submitted our completed reports for official agency comment. Therefore, while it is possible that these agency comments may affect our understanding of specific points that we are reporting on today, they are not likely to significantly alter our overall conclusions.

As a result of our review, we found that the practices at the nine agencies in general did not meet our criteria for providing reasonable assurance that appropriate security controls were being successfully incorporated into the development of the nine systems. Moreover, we observed significant problems that were common among the agencies studied, suggesting that these problems might be common to most civilian agencies.

Our most significant finding in this regard is that all nine of the system development projects reviewed made important decisions concerning the overall system architecture without adequate consideration by management of security needs. Furthermore, six of the nine had proceeded to the systems design without adequate consideration by management of important security needs. If they had given adequate consideration of security needs, their basic systems development decisions might well have been influenced.

The early activities of a system development process are focused on the determination of the system's functional requirements and on an identification and assessment of the major design approaches available to meet these requirements. It is considered to be good practice, and within the intent of federal guidance, that agencies go through a formal, documented process to assure that the overall system architecture and the system approach arrived at represent

accountable management decisions that are based on a knowledgeable consideration of the costs and benefits for the range of feasible alternatives.

None of the agencies we reviewed, however, treated information security as one of the system's integral functional requirements. In particular, we found that the agencies were significantly weak in making overall assessments of their systems' potential vulnerability to threats, such as identifying the major security control approaches and conducting initial assessments of the economic, operational and technical feasibility of these approaches. Specifically, six of the nine agencies either did not address, or inadequately addressed, the sensitivity of the information to be handled by the system. Most of the agencies, eight of the nine to be specific, did not perform any analysis of risk to the proposed system. That is, only one of the agencies explicitly analyzed the potential risks to the system. We also found only one attempt at a cost/benefit analysis of security alternatives and that analysis was missing the applicable security benefits.

Later security-related development activities are intended to assure that appropriate security controls are specified, developed and tested. Without a thorough understanding of a system's security requirements and alternatives, however, we believe that the effectiveness of these activities was either nullified or significantly reduced in most of the cases we studied. For example, seven of the agencies had progressed in the system development process to the point of identifying where security controls were to be located in the system. In each of these cases, we judged that agency management could provide no positive assurance that they had appropriately identified the location of controls. The reason, because they could not demonstrate where the systems were vulnerable.

Additional weaknesses were evident in the subsequent security development activities, where some important security-related procedures were not performed at all. For example, three of the four agencies that had reached the construction phase of system development were writing and testing software without plans and procedures to test the security aspects of that software.

We are preparing a report that will document the overall results of our review of agency practices. In addition, we will provide separate reports to each of the nine agencies we studied concerning security development practices for the specific systems under development at their agencies. We also are continuing our analysis of deficiencies in existing government-wide policies, standards and guidelines that may contribute to the observed weaknesses. We are planning to report to you on this subject later this year.

I will close, Mr. Chairman, by saying that there is a need for agency managers to take the initiative in providing security controls during the development of mission-critical sensitive systems. In taking this initiative, agencies have to look beyond literal compliance with existing federal policies, standards, and guidance to treat system security requirements with the same rigor and with the same thorough consideration called for in the treatment of other functional requirements.

Mr. Chairman, this completes my prepared statement. We have brought along some charts, which have been inserted in the record,

which have information specific to the review of the individual systems development projects we studied.

We stand ready, and will be pleased to answer your questions regarding these systems, or regarding our overall system development practices in general. Dr. Podell and Mr. Wyrsch may also have some answers for you.

Mr. GLICKMAN. Thank you, Mr. Giammo. Not a very pretty picture indeed.

One thing I might say to start out with, however, is that perhaps we could go through a couple of these agencies, without going through all nine of the systems, but, you know, in trying to get some specific information as to what you found at the individual agencies you worked with. Why don't you pick a couple at random? The whole thing is going to appear as a part of the record, but let's see what—give me some analysis of a couple of agencies.

Mr. GIAMMO. Let me explain to you how to read the chart first, so that it makes some sense.

What we've done as I've indicated in my statement, that we grouped the activities that take place during the system development process, and we identified the specific activities that are needed to make sure that the security requirements are appropriately considered.

To give you some examples, on that first chart along the left side there, they say Initiation activities. And what we mean by that is, those activities that go on during the agency development process, where the agency determines the overall scope of the system and identifies the major factors that influence the design and implementation of the system.

The kind of activities we talk about going on in those phases that are security related, the things that move to the right of that first initiation line, are those kinds of security related activities where the agency identifies its sensitive data, where it establishes the overall security objectives, analyzes its major risk factors. And the presumption is that in order to make the good decisions regarding the overall structure of the system, and how the system is going to be developed, agencies have to go through these security activities, or else they don't have the right kind of information that they can use to do the right things in the system as a whole.

Similarly, in that second phasedown, the Definition phase, we group together all those activities that are involved when an agency starts developing its very detailed system requirements. And again, we have a list of security related activities that the agency ought to go through to make sure that security is considered as one of those requirements.

Now, what we've done in each of the agencies, is we've gone through and looked at the systems that were actually being developed, and we made some assessment as to whether the activities were being performed in such a way that the managers had the right information at the right time to make the critical decisions relative to the design and implementation of the system. And for shorthand purposes, we divided our assessment into two categories, a very binary yes/no kind of a thing. One is that they're doing it in the right way, what they're doing supports the assurance that they're considering the right things as they're building the controls

of the system. The other broad category is that it reduced assurance. That they're doing something that compromises the ability of the management to be sure that the right things are being put into the system. And further subdivided out of the two other categories, and some of the activities weren't performed at all, which is hard to understand in some cases.

Other cases we wanted to distinguish that where they made a try to accomplish the activity, but weren't fully successful for one reason or another. One factor that's important to note as we go through these, is that if you don't have a good basis to start with, if you start with a misunderstanding of what your security needs, or if you ignore security early in the process, it's very hard to bring it back into the system later on during the design phase and the construction phase. You started on the wrong track, you're designing your modules without the benefit of security, you're building the system without the benefit of those designs, then you're going into tests without having it in the test. So, typically, you'll find as an agency goes through, they may have done some of the initial phases right, but if there are significant problems with the early phases of the systems in terms of ignoring security, the thing just gets worse as it goes down, because the later stages have nothing to build on, nothing to work from.

Do you have any agencies in particular, of the nine, that you'd want us to talk about? Maybe FAA would be one?

Mr. GLICKMAN. Yes. Let's try the FAA.

Mr. GIAMMO. We're being assisted by Ms. Nagy, by the way.

I'll have Dr. Podell recount—Dr. Podell ran the actual audits of these agencies. I'll have him recount the specific finding.

Dr. PODELL. The system that we looked at is the Advanced Automation System. This is the FAA's air traffic control system for tomorrow. It is a mission-critical system. It will involve real time and processing, and has substantial human safety implications.

When we looked at the advanced information system, it was in the definition phase, focusing on security requirements. And that was at the time of our review. Our overall observation in this particular system development is that we are concerned that the FAA will be investing over $4 billion in tomorrow's air traffic control system, without producing assurance that the information security requirements will be effectively incorporated. And that's really what we're showing on this chart.

Let me give you some of the highlights. The FAA has not assessed whether security requirements are feasible and cost effective. We were looking for a formal assessment of this. We observed a serious lack of coordination within the agency itself. In meeting with the agency officials, we found that the following offices were not coordinating on security requirements. The first office is the AAS, the Advanced Automation System Program Office. The second office is the User Requirements Branch in the Air Traffic Control Operation Service, and the third office is the Office of Civilian Aviation Security.

The existing relationships among these organizations does not insure that the security requirements which have already been identified by the security office will be considered and incorporated into this system design for AAS. The two design contractors that

have already performed design competition activities, have performed these activities with incomplete information regarding the security needs for AAS. So, this gives you an overview of our major concern, and as Tom Giammo pointed out, we summarize that in the different columns, in the sense that some of these activities are not performed at all.

Mr. GLICKMAN. Why don't we hold that comment. Let's go vote. These are the second bells. I think that after these bells, we'll be able to come back and be able to finish the hearing in an uninterrupted fashion.

[Recess.]

Mr. GLICKMAN. I'm sorry. You were right in the middle of a——

Mr. GIAMMO. I was going to add a comment.

Mr. GLICKMAN. OK.

Mr. GIAMMO. To bring you back to where we were, sir, we were talking about—finished the discussion of the overall view of FAA, and what I could add is a comment to show you why some of the specific things we found here are perhaps of larger problems that may be occurring at other agencies. I just wanted to draw the general from the specific.

We have an interesting case here at FAA, where the user did not, as you can see from the chart, perform any risk analyses, specific risk analyses, security feasibility studies, or did any cost/benefit analysis in security. The reason, it was felt there, is that they have a lot of background in this and in some sense they thought it was premature, because they didn't know all of the details of the system. It hadn't been decided on at that point, so it wasn't necessarily the right time in their mind to do any formal analysis. Yet, you'll notice that they did produce security requirements. The lack of logic in that I don't think is apparent to them, that you can actually write down security requirements without having done all of that.

Mr. GLICKMAN. What you're saying is that they on paper put down in some sort of a plan what their needs were?

Mr. GIAMMO. Correct.

Mr. GLICKMAN. In terms of security.

Mr. GIAMMO. But, it wasn't based on any analysis that's called for or logically necessary to substantiate those requirements. It was based essentially on their feeling that, well, we're experienced people. We've been in this business a lot. I can directly write down—this at the user level—I can directly write down what the requirements are.

Mr. WALKER. Is there a generic capacity though, in most computer plans and programs that would allow them to suggest that in purchasing a computer system, that they would get certain security requirements simply by purchasing the system?

Mr. GIAMMO. I want to make a distinction. That brings up another important distinction which shows up in some of our other studies. I want to distinguish between the system that the application is going to run on as opposed to the application itself. There are certain kinds of things that you get when you buy—security features that you can buy with a system, a part of the operating system. And, in that respect you're perfectly correct. But, the most important parts are the special controls, the application oriented

controls that have to be built in to respond to specific threats to the data itself, so that people can't enter erroneous transactions, for example, in the transaction oriented system. Those you can't get as general——

Mr. WALKER. Are those program issues or are they hardware issues?

Mr. GLICKMAN. They tend to be program issues. Sometimes you have to rely on special hardware to get them implemented. But deciding what needs to be done, we treat as definitely a program issue. Because there's no generic way of telling by looking at data as to what its sensitivity is. You have to have some program oriented judgement that this data is sensitive. It's liable to be attacked because there are people out there that are interested in it. It's subject to fraud because there are people who can get economic benefit by changing it. Those are judgmental concerns and considerations that only the program oriented people, the users, can put into it. And if they don't systematically go through and analyze these things, if management doesn't see an analysis like that, they can't make the trade-offs.

Security is expensive. You never can achieve perfect security. So you're constantly making decisions as you're designing a system that bring reality back in with what might be ideally suited. And without having the trade-off analysis in front of you, without having the pros and cons on both sides, you have no idea whether you're appropriately choosing the level of security.

Now, I would probably feel less concerned if the arrow tended to be on the side of being overly secure, you know, spending more money than was necessary. That would be a different kind of a problem. But, what you see in all of the cases we've seen, the tendency tends to be exactly the other way. It tends to be nobody's problem, and it tends to be ignored. Decisions that are made are made off the cuff, and they tend to be ones that tend to shortcut security rather than over emphasize security.

And I guess the major message we're trying to get through in the report is that this is a decision process that has to be explicitly management, have explicit management consideration. You can't have it done by GS 11's and 12's who are in the development team, who decide that they don't need to do a certain kind of feature, put a certain kind of control in the system because they didn't need it last year, or because this is just an automation of a manual system and we didn't have it in the manual system. You've got to bring these up to the same level that the other major requirements of a system are subject to.

You go through a formal process when you're building a system, of determining what the requirements are and have user management sign off on, having development management sign off on it. Typically, security isn't a part of that process. And this is why. Because it's not considered to be a symmetric kind of requirement like the other functional requirements are.

Mr. GLICKMAN. Well, that leads to a related question. Why do you think the agencies are doing so poorly in building in the appropriate securities control systems up front in their information systems?

Mr. GIAMMO. It's an elaboration on what I was saying just now, is that it's treated totally as not being a user requirement. It's not an integral requirement of the user. It's something that's done on the side by other people. The real development process that goes on in an agency is between the using organization, the one that the system supports, and the developers. Those are the people that are interacting constantly, deciding what the requirements are, what can be afforded, how it technically can be implemented. Security is not part of that dialogue, typically. Security is taken off on the side, and if its explicitly approached at all, it's typically done by a security agency, or done informally in the process between the users and the developers. It's not treated in the same kind of formal way that brings management into the process to make decisions as to whether something is too expensive, something is too risky, and so forth.

And that's the major problem that exists. That the procedures, the guidance that we have on the books, the federal guidance we have on the books itself treats security distinct from the other aspects of the system development process. No one has an incentive to bring it into the process. To the developers, it's another thing to worry about. It's something that's very hard to implement and difficult to do. The users think of security as being a burden on them. It's something that gets in the way of their function, as opposed to something that's assisting their function. And the poor security officer, when he's involved, is off on the side and organizationally distinct from the developers and from the users and typically has very little to do with this. That's very much indicated by this process here that went on in FAA.

They had a very well intentioned security office. They did a very nice security assessment of the system and it sat on the shelf.

Mr. GLICKMAN. The users didn't consider it to be a requirement, and the developers say we only respond to user requirements.

Mr. WALKER. I'm sorry I wasn't here earlier when you went through some of the rest of the agency, but if you looked at some place like at CIA, or NSC, or even Department of Defense, my guess is there that the user does have some desire to build in security, so that you would find a different kind of attitude there, and so therefore this is something that they look at?

Mr. GIAMMO. I would agree.

Mr. WALKER. Okay.

If that's the case then, our problem is in convincing program managers that this is in fact a real concern for them, by making certain that they understand that this is something that has to be discussed as a part of their system?

Mr. GIAMMO. I would go one level—because of the universality of the problem, I would go at least one level higher and say that agency managers have to start thinking of security and its context.

The difference between the DOD agencies and the civilian agencies is that DOD is itself, you know, it's inherently very security conscious. So, it's built into the agency procedures when they write out the system development procedures in the military side, you'll see that's built in. It's considered a part of the entire development process.

Mr. WALKER. But, we're dealing with an attitudinal problem?

Mr. GIAMMO. Partially with an attitudinal problem, yes. And I think you have to go to the level of the agency or I would suggest even you go to the OMB, GSA, NBS level, to start laying out some good guidelines for these people to follow.

I had someone call me——

Mr. WALKER. Well, but that's where I'm troubled. You may lay out the guidelines, but if you don't change the attitudes, you know, the fact is that if the guidelines exist they will still be ignored as much as possible, is what I'm getting from this discussion. If in fact DOD and CIA and a lot of these people that feel very strong that they've got to have security, they build it into their systems. If we don't convince other people along the line that they've got to build it into their systems too, they will find a way to ignore it.

Mr. GLICKMAN. I gather, though, what you're saying is we have nothing now. We have no guidelines nor attitudes.

Mr. GIAMMO. You have neither. Both are very, very important pillars that you've got to build on.

As I was going to say, I had someone call me, a contractor from a civilian agency, when we started this job— it was coincidental. And he said, my agency was audited a couple of years ago by GAO, and found that we didn't do a good job in security. I'm the program manager. I want to do a good job. What do I do, so I don't get banged by you people when you come back in three or four years and he said point me to some documents to follow. And I couldn't find any documents for him that I could point to. I could show him the mass of federal guidance, and say it's in there somewhere, and most of its in there, but not all of it, and when on further looking on it, some parts really weren't in there. And that's one of the things I think attracted me to the committee request, because I saw this was an important need that was being overlooked, that we're not getting good guidance from the central agencies that allow a good intentioned manager, in that case a contractor, to do a job that would be considered satisfactory. So, you know, I gave him some fatherly advice and sent him on his way so-to-speak.

I was impressed though. I could not point to any sort of documentation that was——

Mr. GLICKMAN. Specifically with FAA, since this committee and subcommittee have some jurisdiction there, you mentioned a lot of theys in the security, are you talking about the FAA, or are you talking about, for example, Martin Marietta, as they run the AAS plan? Who are we talking about?

Mr. GIAMMO. We're talking about agency officials themselves. These are government employees, part of the FAA itself. We're not talking about the contractor. This is at the level where they're determining the requirements that are being given to the contractors, as opposed to the contractors in trying to implement and execute those requirements.

Dr. PODELL. The offices that we met with are the Advanced Automation System Program Office, and they were really the key spokesmen in regards to this discussion. Their view was——

Mr. GIAMMO. They were the develcpers.

Dr. PODELL [continuing]. We're putting together a system. The users were not at this meeting. This is the Air Traffic Operations Service were not represented at the meeting, and the position of

the program office was, unless the Air Traffic people came with specific security requirements, they would not consider any of the security studies that we had just mentioned that were done by the security office.

Mr. GIAMMO. That's the Office of Civilian Aviation Security, had done those studies.

I didn't get a chance to point out, or maybe I did in the prepared statement, that we are preparing nine individual reports addressed to the specific problems we saw at each of the individual agencies. And in those reports we intend to make specific recommendations to the individual agency how some of the problems might be addressed that we observed.

Now, in the one on the FAA, we are intending to address that problem about how some organizational changes are necessary to assure that security is being considered. Especially when they have an office that's doing security studies, that that get into the development process somehow.

Mr. GLICKMAN. We went through the FAA and the INS. Let's go to another example that—Social Security?

Mr. GIAMMO. Social Security, that would be fine, sir, but we had picked IRS as being an excellent example of having another general problem.

Mr. GLICKMAN. Okay.

IRS, Automated Examination System. This is the one that what, picks our returns on some sort of computerized basis to audit?

Dr. PODELL. It's actually a field automation system to support the audit and examination function.

Mr. GLICKMAN. Okay.

Dr. PODELL. So we'll again give you some of the basic background and this is for the chart that's up here on the IRS.

This is the Automated Examination System. It is mission-critical. It supports tax audits and tax auditors, as well as the revenue agents. It's essentially bringing automation to them in the field in the field of micro-computers. It would be processing sensitive taxpayer data, and this data would be protected by the Privacy Act, as well as the IRS Code.

The AES was in the definition phase, developing system requirements at the time of our review, and that gives you a status of where it was. Our concern is a slightly different concern than what we have shared with you on the FAA. We found that IRS did not perform analyses, critical security analyses. They commented that these analyses were not performed under the assumption that they were automating an existing manual examination process, and therefore IRS was reasoning that they were exempted from the security analysis for the automated system. What we have here is a very profound issue, that their audits in the field and reviews in the field are being done manually, and they feel whatever security procedures they have are implicitly acceptable as they go into the automated tools, the automation. The review process in the field where they could very possibly have new risks that do not exist in the manual system.

Mr. GIAMMO. Again let me add, this point we ran into more than one occasion where they had another system that in some sense served as the model for the automated system. In one other case

we had where they were changing from one automated version to another automated version. And the assumption was, was that all the thinking about security had been done previously when either their manual system had been designed, or when the first automated system had been built. And that it wasn't necessary to explicitly think through this again.

I think the most egregious case is the IRS one, because they're going from a folder oriented, paper, manual system, to something where the form of the data is going to be in an electronic form. And it doesn't take much to realize that it's subject to different kinds of threats, just on—you could walk out, potentially walk out of the office with hundreds of folders worth of data on a small floppy disk, whereas it would be a little bit less likely that you'd walk out with all those folders under your arm.

And another point I'd like to make, we're not saying necessarily that they've arrived at the wrong requirements, but we don't know whether they have or not. And I think that's an important point to drive home, that they can give no assurance that they thought through the threats that have to do with the automation And they leave it to us to prove to the contrary. And I think that's really a basic, one of the fundamental floors here, the attitude of the developer has to be right. He doesn't have to show his management, he doesn't have to show external folks that he's done a good job, that you have to trust it is done and you have to prove the contrary. And I think we have to turn that attitude around too, in the long term, is that the developer, as part of the development process ought to produce positive assurance that the procedures he's following are likely to result in good controls.

And here's a case where you just can't tell. The media totally changed, the way things are done have totally changed since being automated, and yet they've done no analysis to indicate why they're not doing anything differently in the security area.

Mr. GLICKMAN. OK.

Mr. GIAMMO. The next one we had chosen was the Immigration and Naturalization.

Dr. PODELL. That should be the first one.

Mr. GLICKMAN. Yes, it is.

Dr. PODELL. This particular system of the Adjudications Casework System is also mission-critical, and it supports the immigration benefit applications process. And as such, that means there's a lot of sensitive information in there, a lot of personal information. It's primarily non-citizens, however, there's personal information regarding citizens and legal permanent residents. And also, some of the data is protected by the Privacy Act.

When we looked at the system, the INS had elected to abandon this particular system and it will have to be redone again. So, this is a very special opportunity to suggest lessons learned from what we have found in this review, and that would apply to their next design.

The overall conclusion we had in looking at the INS is that they were not performing key security activities in the very beginning of their development, what we call the initiation phase. Therefore we had no assurance that INS was developing effective security specifications during the design phase for this particular system.

It's essentially building the foundation for a building. It's like not having a basement, not having a foundation and you start with the second floor.

Mr. GIAMMO. One of the things I point to here, is that they're at least trying in some of the areas. They at least have a concept that these functions ought to be performed. I think we're concerned mainly that they have to be stiffened up, so that they'll be made more sound, and done better. And as Dr. Podell pointed out, the fact that they have abandoned the current development efforts and are restarting, for reasons that are only partially related to this, it gives them an opportunity, I think, to consider some of these. And we're going to make in our report to them, some specific recommendations, how they ought to modify their procedures as they redesign and redevelop the system, so as to pick up some of these points that we're making here.

Mr. GLICKMAN. All right.

Mr. GIAMMO. And the last one we chose for the short version of the tour of the agencies was the U.S. Customs Service.

Mr. GLICKMAN. Do me a favor. Let's not do customs now. Let's do Farmers Home Administration, because I'm on the Agriculture Committee.

Dr. PODELL. Conceptually, this case is virtually identical to INS. The Farmers Home is the Automated Program Delivery System, APDS. This is a mission-critical system that supports loan and grants programs in the agricultural community. It processes sensitive financial and profile information. I'm talking about a lot of money here. Also there is data protected by the Privacy Act.

We evaluated APDS during the initiation and definition phase. Our concerns after we did this evaluation is that we found that Farmers Home was not really defining an effective mix of security controls in the definition phase for the APDS, and our concern is that Farmers Home didn't do some of the basic security feasibility, cost and benefits of security alternative analysis. And as a result that these weaknesses were apparently continued in the design, including security requirements.

In a case very similar to INS, this particular contract was abandoned in a contractual sense. So we feel the Farmers Home also has an opportunity for lessons learned from our results as they rebuild this system.

Mr. GLICKMAN. Well, you said they have an opportunity. Do you have any reason to believe they're going to take advantage of your recommendations?

Mr. GIAMMO. I don't think we have reason either way. We haven't discussed these formally with agency management. The kind of contacts we've had with the agency up to now have been on an informal level, typically with the developers of the system, where we check the factual aspects as to whether things were performed or not performed according to certain criteria. We have just begun—we have only, I think, two agencies that we have any formal written comments from. We're going to go out formally now, on all nine of these to get top agency management response. I think at that time we'll get an understanding as whether they intend to follow the recommendations or not.

Mr. GLICKMAN. All right.

When you get these responses, I presume that you will—are you going to prepare an additional report?

Mr. GIAMMO. We're preparing nine additional reports, one for each of the nine agencies, which we'll issue separately.

And we intend to have that within the next four to six weeks.

Mr. GLICKMAN. Okay.

Mr. GIAMMO. Excuse me. It will be longer than that. It will be about six to ten weeks. I'm sorry.

Mr. GLICKMAN. Make sure you let us know if you're having any difficulty getting any of this information.

Mr. GIAMMO. Yes, sir, we will.

Mr. GLICKMAN. We can perhaps help in that regard.

Do you have any beliefs, any judgments as to which agency in this government, you think has the greatest computer security problems?

Mr. GIAMMO. That's a hard—it's overwhelmed with choices at this point. It would be hard to say which has the most problems. I think of the civil agencies we looked at, none of them are doing what I would say is an acceptable job in this regard. As you said, I think Mr. Walker said earlier, some of the military agencies are doing a lot better job. And I think we've seen some guidance documents from NASA, which I guess is on the other—not a civil agency in the usual sense. They're very, very security conscious during the developmental process.

But in terms of the kinds of things we're looking at here, I think there are serious problems at all of the agencies we looked at. I don't think we have any particular that we would single out as being necessarily the worst.

Mr. GLICKMAN. Have you had a chance to look at the bill, H.R. 145, the Computer Security Act?

Mr. GIAMMO. Yes. I supported the testimony for that in front of the House Government Operations Committee.

Mr. GLICKMAN. As you know, we are—that bill has now been reported out of Government Operations. We are going to try to report it out tomorrow. I wonder if you might have any comments about how you think this bill might improve existing federal guidelines on how to incorporate security into a design system, the attitudinal thing, as well as the program side of the thing.

Mr. GIAMMO. I read only the original draft. I don't know how it's been modified in the various committee hearings. But in terms of the original drafts that I read, I think it will have a very beneficial effect.

One thing, it focuses security as an issue very strongly, and it really brings the fact that it's a matter of Congressional concern. Secondly, I think it strengthens the NBS role considerably, even though NBS has had a role, it's been a shadow role that hasn't really gotten the kind of support that I think it needs. By giving the accountability so strongly to NBS, for developing the full range of security guidance, I think you put an increased obligation on them to do a better job in this area and maybe strengthen them a little bit in the appropriations process in terms of showing a need to get increased expertise in this area.

So while I don't think it will cure all of these problems, it more needs to be done beyond the passage of H.R. 145. I think it lays a

foundation, at least, where you begin to get the right kind of focus and you get the right kind of people involved.

Mr. GLICKMAN. Let me ask you a question away from that.

If somebody asked you how many agencies you think it would be possible for a computer hacker to break into using an ordinary home computer, how would you respond to that question?

Mr. GIAMMO. Without actually studying it, it would be hard to say, because it would depend on how the specific systems were laid out.

I'll give you a different answer maybe, and see if that's—I don't consider that to be the most serious problem faced by the agencies. A hacker can come in and do sort of miscellaneous damage, you know, typically—I'm not saying they can't do worse damage than that, but I think you'd find if a study was done, that the more serious damage, I mean the dramatic, purposeful damage, is done either by current employees or by ex-employees. People who have a detailed knowledge of the internal workings of the system, and can get by the first level kinds of checks and balances that have been put into the system. And those are the ones that I think that we're—those are the ones you don't find as often, because hackers, because they're tumbling around in the system tend to get caught. The more sophisticated people who know how the system are being protected, if they're being protected at all, and know how to rip them off with some precision, those are the ones that either don't get caught, okay, or when they're caught they don't publicize them because there are such massive intrusions into the system.

So, if I were going to protect a system, and I think one of the reasons why we put so much emphasis on the formality of this, is to make sure that the system is designed well from the inside out, so that you identify the fact that you have a certain class of employees, systems programmers for example, who have a lot of access to elements of the system. And you have to protect against them too. You have to worry about whether they're cleared, and you have to worry about all sorts of things about whether they have the right kind of controls placed on their access to the system. And those are subtle, complicated things, and if you don't get a formal process to do that, I think you potentially miss some of the most damaging threats to the system.

Mr. GLICKMAN. Over the past couple, three years or so, you've been looking at this thing for awhile. Have you seen any improvement?

Mr. GIAMMO. Well, I guess if we fished for awhile, we can find some minor improvements. I think some of the technology is getting a little bit better and there's been some, I guess improvements in that sense. But, by and large, no. And I think the improvements in the system are not growing as rapidly as the threats to the system are. Because we're getting more and more involved where federal systems are becoming the heart of how an agency operates. They're becoming more and more depending on automated decision making in various ways, and integration of large amounts of data across the entire range of the systems activities, and the vulnerability to threat has gone up considerably, I'd say over time. And any increase in sophistication on the defensive side, in the building in of security controls, I think has failed to keep pace with the

magnitude of the vulnerability that's occurred because of the increased use of computers and the essence of federal government.

What's especially disturbing about this study that we've come up with, is the fact that the systems we're talking about here, the nine in particular, but all the other ones that are being built now, they're going to be around until the year 2000, and then some. And it's disturbing that the only time that you're going to find—if they were to continue to be built the way we've seen them built, the first time security will be seriously considered, I mean in the sense of a real rigorous approach to security, will be after the first penetration and failure is discovered. Then the agency will run around and decide how they can retrofit back into the system the security controls that probably should have been considered, and could have been considered at the time they were being built.

And what you're seeing—what they're doing here, is there building reasons for you to have hearings 10 years from now, as penetrations occur in the systems that are under construction now. And that's what's very discouraging, because you're not going to get an improvement by retrofitting old systems. That's very hard to do, very technically difficult and very, very expensive. Where you're going to see an improvement is a slow improvement as you get better quality systems on line, that are built from the bottom up with security in mind. And what's discouraging about what we've seen, is you don't see that happening. Security is still the same degree as an afterthought as it was when the systems that are in operation today were built.

Mr. GLICKMAN. Well, I think hopefully, H.R. 145, if it becomes law, will increase the sensitivity. And while it's been subject to a little bit of controversy as to who runs the show, the idea is to create and heighten Congressional interest and also ensure that as the systems are built, and as they're implemented into the system that security is part and parcel of the whole thing.

In law school, I recall that there was a judge—I can't think of his name, but it was a famous case in defining negligence, and they defined it the risk to be perceived defines the duty to be obeyed. And the risk to be perceived in this whole area is just monumental, incredible risks to everybody's personal lives, as well as national security issues, and you know, banking system, and FAA air traffic system, and down to basic entitlement and human related programs. And the duty has been very small, very minimal, not very important at all. That's what we're trying to do is to highlight this issue the best we can.

We appreciate your work and look forward to your specific reports on the nine agencies that you're looking at, and I don't know whether we'll have another hearing or not, but I'd have to talk to the Chairman of the subcommittee on that, but we're going to continue to pursue this issue and do oversight, even if we are successful in passing this legislation.

So I appreciate your testimony today. Thanks very much.

Mr. GIAMMO. Thank you.

Mr. GLICKMAN. It was Judge Cardoza who said that.

Mr. GIAMMO. I'd have to refer to my lawyer, Mr. Wyrsch, for comment on that. I'm not capable.

Mr. GLICKMAN. Benjamin Cardoza.

The subcommittee is adjourned.

[Whereupon, at 3:41 p.m., the subcommittee was adjourned.]

[The prepared statement, plus charts submitted by Mr. Giammo follows:]

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE: We are pleased to be here today to provide the Subcommittee information on our review of the practices used by federal civilian agencies in identifying and incorporating appropriate security controls in automated information systems. I have with me Dr. Harold J. Podell, Group Director from the Information Management and Technology Division, and Mr. Raymond J. Wyrsch, Senior Attorney from our Office of General Counsel.

Mr. Chairman, the work we are reporting on today is a follow-on to the review of the security for information systems at 17 agencies that we performed at the request of this Subcommittee in 1985. In that work, we examined the security of 25 automated information systems that had already been put into operation. We identified significant deficiencies in the controls of those systems that exposed them to abuse, destruction, error, fraud, and waste. An important finding of that work was that the origin of some of these deficiencies could be traced back to the development of the systems: appropriate security controls had not been successfully incorporated into many of the system at the time they were planned, specified, and built.

Our present review is in response to a July 30, 1985, request from the Chairman of the Committee. We were requested to review how well civilian agencies are currently assuring that appropriate security controls are being successfully incorporated into their mission-critical, sensitive systems that are now being developed.

Mr. Chairman, our review suggests that the practices currently being used by civilian agencies in the development of mission-critical, sensitive systems will not assure that the appropriate security controls are being successfully incorporated into these systems. Specifically, we reviewed the practices currently being used at nine civilian agencies in the development of nine specific systems. We found that the practices in use at all nine agencies had permitted decisions critical to the specification, design, and construction of all nine systems to be made without adequate management consideration of important security issues.

Consequently, we believe that the systems currently in development at many civilian agencies (and intended to be used at least through the 1990s) are likely to possess many of the same security deficiencies we had previously found in the older systems already in operation. There is sufficient reason for concern that automated information systems of the future are likely to be only marginally better secured than those of the current generation. There is even more reason for concern, however, when one realizes that the automated information systems being developed today are likely to play an increasingly significant role in the essential business of our civilian agencies.

I would like to address the basis for these observations in greater detail, Mr. Chaiman.

INFORMATION SECURITY

Criteria

We began our review by surveying existing federal guidance relating to the practices that should be used in the development of federal information systems. On the basis of our initial analysis, we concluded that the body of existing guidance was not a suitable basis for assessing whether agency practices provided appropriate security controls during the development of systems. Most of the relevant civilian guidance addresses general aspects either of the development process or of security concerns—little effective guidance exists that comprehensively addresses how an agency should incorporate security considerations into the system development process. This absence in itself is a significant finding. We believe that this lack of specific federal guidance is an important contributing cause of the universality of the problems we found in this area. Therefore, rather than relying exclusively on the letter of existing federal guidance as the basis of our evaluation, we explicitly formulated our own criteria by applying the general principles given in that guidance to the specific activities needed to build security into an automated information system. In doing so, we followed accepted system development procedures.

The essence of these criteria turns out to be just common sense—we believe that agency management must consider security requirements and constraints when making critical decisions about overall system architecture, detailed design, testing, and implementation. Simply put, for each of the critical decision points in the development of an automated information system, we identified important security-relat-

ed information that management should have prior to making those decisions. In our review, we checked to see if this information was available to management and if it was considered in reaching the critical system development decisions. Unless we had positive evidence of this, we judged that agency management's ability to assure that appropriate security controls were being incorporated was significantly reduced.

Not surprisingly, the criteria we used corresponds to the "good practices" set out in several individual agency guidance documents and a draft report of the President's Councils on Management Improvement, and on Integrity and Efficiency.

AGENCY PRACTICES REDUCE ASSURANCE THAT APPROPRIATE SECURITY CONTROLS ARE SUCCESSFULLY INCORPORATED

We reviewed the practices currently being used at nine agencies in the development of nine specific mission-critical, sensitive systems. (I will submit for the record the identification of the nine agencies and the systems studied.) We solicited informal agency comment from responsible officials on our findings at each agency. We received comments from seven of the nine agencies. We have not, however, yet submitted our completed reports for official agency comments. While it is possible that these agency comments may affect our understanding of specific points that we are reporting on today, they are not likely to significantly alter our overall conclusions.

As a result of our review, we found that the practices at the nine agencies in general did not meet our criteria for providing reasonable assurance that appropriate security controls were being successfully incorporated into the development of the nine systems. Moveover, we observed significant problems that were common among the agencies studied, suggesting that these problems might be common to most civilian agencies.

Developing An Information System Security Foundation

Our most significant finding is that all nine of the system development projects we reviewed made important decisions concerning the overall system architecture, and six of the nine proceeded to system design without adequate consideration by management of security needs. Consideration of security needs might have influenced these basic system development decisions.

The early activities of a system development process are focused on the determination of the system's functional requirements and on an identification and assessment of the major design approaches available to meet these requirements. It is considered to be good practice (and within the intent of federal guidance) that agencies go through a formal, documented process to assure that the overall system architecture and the system approach arrived at represent accountable management decisions that are based on a knowledgeable consideration of the costs and benefits for the range of feasible alternatives.

None of the agencies we reviewed, however, treated information security as one of the system's integral functional requirements. In particular, we found that the agencies were significantly weak in making overall assessments of their systems' potential vulnerability to threats, such as identifying the major security control approaches and conducting initial assessments of the economic, operational, and technical feasibility of these approaches. Specifically, six of the nine agencies either did not address, or inadequately addressed, the sensitivity of the information to be handled by the system. Most of the agencies (eight of the nine) did not perform any analysis of risk to the proposed system. That is only one of the agencies analyzed the potential risks to the system. We also found only one attempt at a cost/benefit analysis of security alternatives and that analysis was missing the applicable security benefits.

INITIAL INFORMATION SECURITY PROBLEMS HINDERED SUBSEQUENT DEVELOPMENT

Later security-related development activities are intended to assure that appropriate security controls are specified, developed, and tested. Without a thorough understanding of a system's security requirements and alternatives, however, we believe that the effectiveness of these activities was either nullified or significantly reduced in most of the cases we studied. For example, seven of the agencies had progressed in the system development process to the point of identifying where security controls were to be located in the system. In each of these cases, we judged that agency management could provide no positive assurance that they had appropriately identified the location of controls, because they could not demonstrate where the systems were vulnerable.

Additional weaknesses were evident in subsequent security development activities, where some important security-related procedures were not performed at all.

For example, three of the four agencies that had reached the construction phase of system development were writing and testing sofware without plans and procedures to test security.

We are preparing a report that will document the overall results of our review of agency practices. In addition, we will provide separate reports to each of the nine agencies we studied concerning security development practices for the specific systems under development at their agencies. We also are continuing our analysis of deficiencies in existing governmentwide policies, standards, and guidelines that may contribute to the observed weaknesses, and we are planning to report to you on this subject later this year.

I will close by saying that there is a need for agency managers to take the initiative in providing security controls during the development of mission-critical, sensitive systems. In taking this initiative, agencies have to look beyond literal compliance with existing federal policy, standards, and guidance to treat system security requirements with the same rigor and thorough consideration called for in the treatment of other functional requirements.

This completes my prepared statement. We have brought along information regarding our review of the nine specific system development projects we studied. We will be pleased to answer your questions regarding these systems or regarding system development practices in general.

CHARACTERISTICS OF SYSTEMS SELECTED FOR REVIEW

AGENCY	SYSTEM/SUBSYSTEM REVIEWED	PHASE OF DEVELOPMENT DURING REVIEW	AGENCY ESTIMATE OF LIFECYCLE COST/a
Immigration and Naturalization Service	Adjudications Casework System	Design /b	$697,000 /c
Farmers Home Administration	Automated Program Delivery System	Definition /b	$7.9 million /d
U.S. Customs Service	Automated Commercial System/Selectivity Module	Testing	Cost estimate not available. System to process approximately $14.7 billion in revenue per year.
Veterans Administration	Decentralized Hospital Computer Program/Blood Bank and Security Kernel Modules	Construction	$42.95 million
Federal Aviation Administration	Advanced Automation System	Definition	over $4 billion
International Trade Administration	Commercial Information Management System	Design	$42 million
Social Security Administration	Claims Modernization Program/Release 3.1	Construction	$56.3 million for software development/e
Internal Revenue Service	Automated Examination System	Definition	over $1.1 billion
Department of Energy	Strategic Petroleum Reserve System	Construction	$25.45 million for hardware and software conversion

a/Agency cost estimates were not reviewed by GAO, and are not comparable.

b/First development effort reviewed. Agency terminated first effort at this phase, and is re-evaluating system development.

c/Cost of first development effort, until terminated.

d/Estimated cost of first development effort, had it been complete.

e/Includes a limited amount of software necessary for software testing. Does not include hardware costs.

ASSESSMENT RESULTS

Immigration and Naturalization Service (INS) Adjudications Casework System (ACS)

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION	• Overall system concepts • Security objectives	• Risk analysis • Security framework	• Sensitive information • Security feasibility • Security cost/benefit	
DEFINITION		• Security requirements • Where security requirements apply • Preliminary security test plans	• Change control • Internal audit plan • Updated risk analysis • Mix of controls • Contingency plans	
DESIGN		• Security specifications [a]		

a Security activities beyond security specifications were not assessed because ACS had not proceeded beyond this point in development at the time of our review.

ASSESSMENT RESULTS

Farmers Home Administration (FmHA)
Automated Program Delivery System (APDS)

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION	• Overall system concepts • Security objectives	• Risk analysis	• Sensitive information • Security feasibility • Security cost/ benefit • Security framework	
DEFINITION		• Change control • Internal audit plan • Security requirements • Where security requirements apply • Mix of controls	• Updated risk analysis	• Contin-gency plans[a]

[a] Security activities beyond developing contingency plans were not assessed because APDS had not proceeded past this point in development at the time of our review.

ASSESSMENT RESULTS
U.S. Customs Service
Automated Commercial System (ACS)

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION		• Overall system concepts • Security objectives	• Sensitive information • Risk analysis • Security feasibility • Security cost/benefit • Security framework	
DEFINITION		• Change control • Security requirements • Where security requirements apply • Contingency plans	• Internal audit plan • Updated risk analysis • Mix of controls • Preliminary security test plans	
DESIGN			• Security specifications • Security test plans	
CONSTRUCTION	• Program library • High-level language • Debugging techniques	• Top-down programming • Unit security testing		

ASSESSMENT RESULTS
U.S. Customs Service
Automated Commercial System (ACS), Continued

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INSTALLATION, INTEGRATION, & TESTING	• Security code installed in "real" environment	• Configured software security test • Integrated system test of security functional operation • Integrated system, test of critical failures resolved • User manual	• Configured network security test • Configured hardware security test • Integrated system test of security performance • Security testing follows plans • Security test results analyzed • Operations manual • Maintenance manual • Acceptance test of security functional operation, performance, and penetration resistance • Security test results evaluated • Certification • Accreditation	

ASSESSMENT RESULTS

Veterans Administration (VA)
Decentralized Hospital Computer Program (DHCP)
Blood Bank and Security Kernel

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION		• Sensitive information • Overall System concepts • Security objectives • Security framework	• Risk analysis • Security feasibility • Security cost/benefit	
DEFINITION		• Change control • Security requirements • Where security requirements apply • Contingency plans	• Internal audit plan • Updated risk analysis • Mix of controls • Preliminary security test plans	
DESIGN			• Security specifications • Security test plans	
CONSTRUCTION	• High-level language • Debugging techniques	• Top-down programming • Unit security testing [a]	• Program library	

[a] Security activities beyond unit testing were not assessed because the DHCP Blood Bank Module had not proceeded past this point in development at the time of our review.

ASSESSMENT RESULTS

Federal Aviation Administration (FAA)
Advanced Automation System (AAS)

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION	• Overall system concepts • Security objectives	• Sensitive information • Security framework	• Risk analysis • Security feasibility • Security cost/benefit	
DEFINITION	• Change control	• Security requirements[a]	• Internal audit plan	

[a] Security activities beyond security requirements were not assessed because AAS had not proceeded past this point in development at the time of our review.

ASSESSMENT RESULTS

International Trade Administration (ITA) Commercial Information Management System (CIMS)

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION	• Sensitive information • Overall system concepts • Security objectives	• Security framework	• Risk analysis • Security feasibility • Security cost/benefit	
DEFINITION		• Change control • Security requirements • Where security requirements apply • Mix of controls • Contingency plans	• Internal audit plan • Updated risk analysis	• Preliminary security test plans
DESIGN		• Security specifications		• Security test plans[a]

a Security activities beyond security test plans were not assessed because CIMS had not proceeded past this point in development at the time of our review.

ASSESSMENT RESULTS

Social Security Administration (SSA) Claims Modernization Program (CMP) (Release 3.1)

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION	• Security objectives	• Sensitive information • Overall system concepts • Security feasibility	• Risk analysis • Security cost/ benefit • Security frame-work	
DEFINITION	• Internal audit plan	• Change control • Security requirements • Where security requirements apply • Mix of controls	• Updated risk analysis • Contingency plans • Preliminary security test plans	
DESIGN		• Security specifications	• Security test plans	
CONSTRUCTION	• High-level language • Debugging techniques	• Top-down programming	• Program library	• Unit security testing [a]

[a] Security activities beyond unit security testing were not assessed because CMP/Release 3.1 had not proceeded beyond this point in development at the time of our review.

ASSESSMENT RESULTS

Internal Revenue Service (IRS)
Automated Examination System (AES)

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION	• Sensitive information • Overall system concepts • Security objectives	• Security framework	• Risk analysis • Security feasibility • Security cost/benefit	
DEFINITION	• Change control • Internal audit plan	• Security requirements [a]		

a Security activities beyond defining security requirements were not assessed because AES had not proceeded beyond this point in development at the time of our review.

ASSESSMENT RESULTS

Department of Energy (DOE)
Strategic Petroleum Reserve (SPR)

Phase	Supports Assurance	Reduces Assurance		In Progress
		Performed	Not Performed	
INITIATION	• Sensitive information • Security objectives • Risk analysis	• Security cost/ benefit • Security framework	• Security feasibility	
DEFINITION	• Change control • Contingency plans	• Security requirements • Where security requirements apply	• Internal audit plan	• Updated risk analysis • Mix of controls • Preliminary security test plans
DESIGN			• Security specifications	• Security test plans
CONSTRUCTION	• Program library • High-level language • Debugging techniques [a]	• Top-down programming		

[a] Security activities beyond debugging techniques were not assessed because SPR had not proceeded beyond this point in development at the time of our review.